HP Network Node Manager iSPI for MPLS

Software Version: 10.10
for the Windows® and Linux® operating systems

Deployment Reference

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2008-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

Intel®, Intel® Itanium®, Intel® Xeon®, and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat® Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries.

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

This product includes software developed by the Apache Software Foundation. (http://www.apache.org).

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **https://softwaresupport.hp.com**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Or click the **Register** link at the top of the HP Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **https://softwaresupport.hp.com**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Introducing the NNM iSPI for MPLS

HP Network Node Manager for MPLS Software (NNMi iSPI for MPLS) helps you to extend the capability of HP Network Node Manager i Software (NNMi) to monitor MPLS services configured on the network.

You can plan the deployment of the NNM iSPI for MPLS based on how NNMi is deployed in the environment. While planning the deployment, consider the following areas to achieve an optimum performance of the system:

- Scale of MPLS objects
- Deployment of the NNM iSPI for MPLS in a High Availability (HA) environment.
- Deployment of the NNM iSPI for MPLS in an Application Failover environment
- Deployment of the NNM iSPI for MPLS along with other iSPIs (NNM iSPI for IP Multicast, NNM iSPI Performance for QA, RAMS, and NNM iSPI Performance for Metrics/ NPS).
- Deployment of the NNM iSPI for MPLS in a Global Network Manager (GNM) environment.

Preparing for Deployment

Before you start deploying the NNM iSPI for MPLS, you must plan the installation based on your deployment requirements. You must identify the ideal deployment scenarios for the supported configuration and make sure that all the prerequisites are met before you begin the installation process.

Factors that impact the deployment of the NNM iSPI for MPLS include the type of database configured with NNMi and the size of the network that you want to monitor. In addition, make sure to install the latest NNMi patches before installing the NNM iSPI for MPLS.

To install and configure the NNM iSPI for MPLS in an HA and application failover environment, see the HA and Application Failover section of *NNMi Deployment Reference Guide.*

Read the following NNMi documents before you start installing and configuring the NNM iSPI for MPLS:

- *HP Network Node Manager i Interactive Installation and Upgrade Guide*
- *HP Network Node Manager i Deployment Reference*
- *HP Network Node Manager i Ultimate Release Notes*
- *HP Network Node Manager i Ultimate Support Matrix*

In addition, read the following NNM iSPI for MPLS documents before you start deploying the NNM iSPI for MPLS:

- *HP Network Node Manager Smart Plug-in for MPLS Installation Guide*
- *HP Network Node Manager i Ultimate Release Notes*

- *HP Network Node Manager i Ultimate Support Matrix*

For current versions of all documents listed here, go to:
http://h20230.www2.hp.com/selfsolve/manuals.

Environment Variables Used in the NNM iSPI for MPLS Documents

The NNM iSPI for MPLS documents use the following NNMi environment variables to refer to file and directory locations. The default values are listed here. Actual values depend upon the selections made during NNMi installation.

NNMi installation process creates the following system environment variables, so they are always available to all users:

- On Windows Server 2008,

  %NnmInstallDir%: `<drive>\YourFolder\HP\HP BTO Software`

  %NnmDataDir%: `<drive>\Yourfolder\HP\HP BTO Software`

  > **Note:** By default, these variables are created in the program files folder on the c drive.

- On Linux,

  $NnmInstallDir: `/opt/OV`

  $NnmDataDir: `/var/opt/OV`

Chapter 2: Deploying the NNM iSPI for MPLS

The NNM iSPI for MPLS and NNMi must be installed on the same management server. To install and configure NNMi on a management server, see the *NNMi Installation Guide and Deployment Reference.*

You can deploy the NNM iSPI for MPLS for the following scenarios:

- Installing NNMi and NNM iSPI for MPLS together on a management server. NNMi and NNM iSPI for MPLS are both configured together.
- Installing the NNM iSPI for MPLS on the management server where NNMi is already installed and configured.
- Installing the NNM iSPI for MPLS in a Global Network Management environment.
- Installing NNMi, NNM iSPI Performance for Metrics/ NPS, and NNM iSPI for MPLS on the same management server.
- Installing NNMi and NNM iSPI for MPLS in a management server and the NNM iSPI Performance for Metrics/ NPS on a dedicated server.
- Installing the NNM iSPI for MPLS with NNM iSPI for IP Multicast, and NNM iSPI Performance for Quality Assurance.
- Integrated with Route Analytics Management Software (RAMS) Appliance.

Deploy the NNM iSPI for MPLS and NNMi Together

To deploy the NNM iSPI for MPLS on a management server, follow these steps:

1. Install and Start the NNMi process.
2. Create a New User with the Web Service Client Role from the NNMi console. For more information, see *Create a New User with the Web Service Client Role* section in the *NNM iSPI for MPLS Installation guide*.

   > **Note:** Make sure to use the same database type (PostgreSQL Embedded or Oracle) as NNMi when you are installing the NNM iSPI for MPLS.

3. Install the NNM iSPI for MPLS, . For more information, see the NNM iSPI for MPLS Installation Guide.
4. Start the NNM iSPI for MPLS processes by using the command: `ovstart -c mplsjboss`.
5. Log on with the administrative privileges to use the `MPLS Configuration` workspace. If you have

the list of Route Targets (RTs) to be excluded in the network, you can add the RTs to be excluded from the `MPLS Configuration` workspace. Similarly, you can group the Pseudowires based on the attributes such as Id or encapsulation type to discover VPWS VPNs. These configurations help in discovering the L3VPNs and L2VPNs.

> **Note:** You can add the list of RTs to be excluded anytime after starting NNM and the NNM iSPI for MPLS processes.

6. Seed the MPLS nodes from the NNMi console. The NNMi discovery process starts after you seed the nodes and MPLS capabilities are discovered along with generic capabilities of a node. For more information, see NNMi Online Help.

7. Log on to the NNMi console and verify that MPLS-enabled nodes are discovered. You can do this using the MPLS workspace. This workspace is visible on the NNMi console after NNM iSPI for MPLS is successfully installed. You can use the MPLS workspace to launch inventory and form views for MPLS objects.

Deploy the NNM iSPI for MPLS in an NNMi Environment

To deploy the NNM iSPI for MPLS on a management server where NNMi is already installed and running, follow these steps:

> **Note:** Make sure to use the same database type (PostgreSQL Embedded or Oracle) as NNMi when you are installing the NNM iSPI for MPLS. Also, to enable LSP management, you must configure device access credentials via SSH or telnet.

1. Install the NNM iSPI for MPLS on a management server where NNMi is already installed, running, and nodes are discovered.

2. Start the MPLS processes. If you have the list of Route Targets (RTs) to be excluded in the network, you can add the RTs to be excluded from the `MPLS Configuration` workspace. Similarly, you can group the Pseudowires based on the attributes such as Id or encapsulation type to discover VPWS VPNs. These configurations help in discovering the L3VPNs and L2VPNs.

3. You can start the NNM iSPI for MPLS discovery process to discover the MPLS objects from the discovered NNMi nodes in any *one* of the following ways:

   - Run the following command to discover the MPLS objects from the discovered NNMi nodes:

     ```
     $InstallDir/bin/nmsmplsdisco.ovpl [ -all | -node <node_name>]
     ```

   - Select NNMi nodes from NNMi inventory and start the configuration poll. For more information, see *Help for NNMi, Launch the Actions: Configuration Poll Command*.

   - Wait for the next NNMi discovery cycle.

4. After installing the NNM iSPI for MPLS, log on to the NNMi console, and then verify the availability of the MPLS workspace and MPLS views.

Inter-Provider VPN for NNM iSPI for MPLS

The NNM iSPI for MPLS provides the following options to users for Inter-Provider VPN, they are:

- "To Turn-on or Turn-off the Inter-Provider Feature." below
- "To Modify an AS Name" below
- "To Turn-Off the LSP feature" below

To Turn-on or Turn-off the Inter-Provider Feature.

Inter-Provider VPN feature is Disabled by default in NNM iSPI for MPLS. To Enable the inter-provider VPN feature:

- Modify `interProviderVPNConfig` file. This file is stored in the following path:

  For Windows:

  `%NnmDataDir%\shared\mpls\conf\interProviderVPNConfig`

  For Linux:

  `/var/opt/OV/shared/mpls/conf/interProviderVPNConfig`

`interProviderVPNConfig` has a global flag to enable or disable the inter-provider VPN feature, along with a list of inter-provider VPNs.

> **Note:** You do not have to restart the mpls jboss after modifying `interProviderVPNConfig` file

To Modify an AS Name

You can modify the Autonomous System name by modifying the `publicASMapping` file. This file is stored in the following path:

For Windows:

`%NnmDataDir%\shared\mpls\conf\publicASMapping`

For Linux:

`/var/opt/OV/shared/mpls/conf/publicASMapping`

To Turn-Off the LSP feature

The LSP feature is enabled by default in the NNM iSPI for MPLS. To disable the LSP feature, follow these steps:

1. Open the `nms-mpls.jvm.properties` file located in the following path:

   On Windows:

   `%NnmDataDir%\shared\mpls\conf`

   On Linux:

```
/var/opt/OV/shared/mpls/conf
```

2. Uncomment the following parameter from the file:

```
com.hp.ov.nms.spi.mpls.lsp.lspFeatureDisabled=true
```

3. Restart the NNM iSPI for MPLS with the following commands:

```
ovstop -c mplsjboss
ovstart -c mplsjboss
```

Using Single Sign-On with NNM iSPI

By default Single Sign-On is disabled. To enable the Single Sign-On feature, follow these steps after installing NNM iSPI for MPLS.

Edit `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`:

1. Set `com.hp.nms.ui.sso.isEnabled = true`

2. Run `nnmsso.ovpl –reload`

3. Run `mplsssoreload.ovpl`

> **Note:** Do not enable Single Sign-On feature when NNMi and the NNM iSPI for MPLS is configured to use Public Key Infrastructure (PKI) authentication.

For more information, see *Using Single Sign-On with NNMi* in *NNMi Deployment Reference.*

Configuring Access with Public Key Infrastructure Authentication

You can configure NNMi to map Public Key Infrastructure (PKI) certificates to the NNMi user accounts. As a result, you can log on to the NNMi console without having to type in the NNMi user name and password on the Login page. However, you will be prompted to provide the NNMi user name and password again when you try to launch the NNM iSPI for MPLS Configuration form, unless you perform additional steps to reconcile the mapping with the iSPI.

When the NNMi is configured to use the PKI authentication, it is mandatory for the NNM iSPI for MPLS to use the PKI authentication.

> **Note:** You can continue to authenticate users with the NNMi user credentials for the NNM iSPI for MPLS Configuration form. However, do not configure only the iSPI to use the PKI authentication when the NNMi continues to use the credentials-based authentication.

Configuring the iSPI to use the PKI authentication involves the following tasks:

- Configuring NNMi
- Configuring a Certificate Validation Method

- Enabling Secure Sockets Layer (SSL) on the NNM iSPI for MPLS
- Configuring the NNM iSPI for MPLS

> **Note:** To configure PKI authentication on the NNM iSPI for MPLS in an HA cluster, you must perform the required configuration tasks on both, primary and secondary node.

Configuring NNMi

To configure NNMi to use the PKI authentication, follow the steps in the *Configuring NNMi to Support Public Key Infrastructure Authentication* section in the *HP Network Node Manager Deployment Reference.*

Configuring a Certificate Validation Method

When NNMi is configured to use the PKI authentication, unauthorized access using invalid certificates must be prevented. You must perform additional steps to configure NNMi to use a certificate validation method—Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

Follow the steps in the *Certificate Validation (CRL and OCSP)* section in the *HP Network Node Manager Deployment Reference.*

Enabling Secure Sockets Layer (SSL) on the NNM iSPI for MPLS

When NNMi is configured to use the PKI authentication, you must enable SSL on the NNM iSPI for MPLS to ensure communication between the NNMi management server and the NNM iSPI for MPLS.

To enable SSL on the NNM iSPI for MPLS, follow these steps:

1. Log on to the NNM iSPI for MPLS.
2. Navigate to the following directory:

   On Windows

   `%nnmdatadir%\shared\mpls\conf`

   On Linux

   `/var/opt/OV/shared/mpls/conf`
3. Open the nnm.extended.properties file with a text editor.
4. Set the value of following properties to true:

   `com.hp.ov.nms.spi.mpls.spi.isSecure`

   `com.hp.ov.nms.spi.mpls.Nnm.isSecure`
5. Save and close the file.
6. Restart the ovjboss process by running the following commands:

   `ovstop -c mplsjboss`

   `ovstart -c mplsjboss`

Configuring the NNM iSPI for MPLS

Configuring the NNM iSPI for MPLS to enable the PKI authentication you must modify the `nms-auth-config.xml` file in the iSPI configuration data directory (`%nnmdatadir%\nmsas\mpls\conf` on Windows; `/var/opt/OV/nmsas/mpls/conf` on UNIX/Linux) based on the updated `nms-auth-config.xml` file. To configure the NNM iSPI for MPLS to use the PKI authentication, follow these steps:

1. Make sure Task 1, Task 2 and Task 3 are complete.

2. Log on to the NNMi management server.

3. Navigate to the following directory:

   On Windows

   `%nnmdatadir%\nmsas\mpls\conf`

   On Linux

   `/var/opt/OV/nmsas/mpls/conf`

4. Open the `nms-auth-config.xml` file using a text editor.

5. Modify the `nms-auth-config.xml` file to enable the PKI authentication. For more information, see *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference.*

   > **Note:** Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

6. Save and close the file.

7. Run the following command:

   On Windows

   `%NnmInstallDir%\mpls\bin\nmsmplsauthconfigreload.ovpl`

   On Linux

   `/opt/OV/mpls/bin/nmsmplsauthconfigreload.ovpl`

The NNM iSPI for MPLS is now configured for PKI authentication.

> **Note:** Do not enable Single Sign-On feature when NNMi and the NNM iSPI for MPLS is configured to use Public Key Infrastructure (PKI) authentication.

The *-u <user>* and *-p <password>* parameters are optional for Command Line Interface (CLI) in the NNM iSPI for MPLS.

Deploy the NNM iSPI for MPLS with the NNM iSPI Performance for Metrics/NPS

You must install NNMi, iSPI of MPLS, NNM iSPI Performance for Metrics/ Network Performance Server (NPS) to view the MPLS reports. You can deploy these products for the following scenarios:

- Installing NNMi, NNM iSPI for MPLS, and the NNM iSPI Performance for Metrics/NPS on the same server.
- Installing the NNM iSPI for MPLS and NNMi on one server and NNM the iSPI Performance for Metrics/NPS on a dedicated server.

To deploy all the products on the same management server, follow these steps:

1. Install NNMi.
2. Install the iSPI Performance for Metrics/NPS. For information about the steps to install, see *HP NNMi iSPI Performance for Metrics/NPS Installation Guide.*
3. Install the NNM iSPI for MPLS.

To deploy NNMi and NNM iSPI for MPLS on the same management server and the NNM iSPI Performance for Metrics/NPS on a dedicated server, follow these steps:

1. Install NNMi and NNM iSPI for MPLS on the same management server.
2. Install the NNM iSPI Performance for Metrics/ NPS on the dedicated server. For information about the steps to install, see *HP NNMi iSPI Performance for Metrics/NPS Installation Guide.*
3. Complete the necessary configurations for NNMi, the NNM iSPI for MPLS, and iSPI Performance for Metrics/NPS.

After you complete the installations, the NNM iSPI for MPLS introduces the following extension packs on the NPS/ Metrics console:

Extension Pack Name	Purpose
MPLS LSR Node	Shows report based on the available metric definitions for all MPLS-enabled nodes.
MPLS LSR Interface	Shows report based on the available metric definitions for all MPLS-enabled interfaces.
L3_VPN_VRF	Shows report based on the available metric definitions for all VRFs and L3VPNs.
MPLS_Lsp	Shows report based on the available metric definitions for all Monitored LSPs.
MPLS_PseudoWire	Shows report based on the available metric definitions for all PseudoWires.
TE_Tunnel	Shows report based on the available metric definitions for all TE Tunnels
MPLS_VFI	Shows report based on the available metric definitions for all VFIs.

The extension packs use data collected by the NNM iSPI for MPLS. Make sure that iSPI Performance for Metrics/NPS is up and running. To view the MPLS reports from the NNMi console, click **Actions-> HP NNM iSPI Performance -> Reporting-Report Menu.** The iSPI Performance for Metrics console appears with the MPLS metrics that enables you to generate the MPLS reports.

After you uninstall the NNM iSPI for MPLS, the extension packs introduced by the NNM iSPI for MPLS are not removed. If the iSPI Performance for Metrics is running, the extension packs introduced by the NNM iSPI for MPLS, still appear. You must remove the extension packs manually before you start installing the NNM iSPI for MPLS again. For more information, see *Troubleshooting the NNM iSPI for MPLS* section from the NNM *iSPI for MPLS Installation Guide*.

Deploy the NNM iSPI for MPLS in an Application Failover Environment

You can configure the NNM iSPI for MPLS in an application failover environment from the following scenarios:

Deploy the NNM iSPI for MPLS in an Application Failover Environment with Oracle Database

Scenario 1: In this scenario, consider that you want to install the NNM iSPI for MPLS with NNMi and then configure application failover on NNMi:

1. Install NNMi in the primary server mode on server 1 and install NNMi in the secondary server mode on server 2.

2. Start NNMi on server 1.

3. Install the NNM iSPI for MPLS on server 1 with Oracle database by following the steps listed in the *HP Network Node Manager i Software Smart Plug-in for MPLS Installation Guide.*

4. Merge the keystores on one server and copy the keystores to both the primary and the secondary servers. For information, see the *NNMi Deployment Reference Guide* for instructions.

5. Install the NNM iSPI for MPLS license on server 1.

6. Stop NNMi on server 1.

7. Start NNMi on server 2.

8. Install the NNM iSPI for MPLS on server 2.

9. Configure NNM iSPI for MPLS on server 2 with the same database instance, user name, and password configured on server 1.

> **Note:** Ignore the warning messages displayed and click **OK**

10. After the installation of the NNM iSPI for MPLS, install the NNM iSPI for MPLS license on server 2.

11. Configure application failover server 1 and server 2 according to the instructions provided in the *NNMi Deployment Reference Guide*.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for MPLS after configuring NNMi in an application failover environment:

1. Remove configuration for application failover from the NNMi primary and secondary servers.

2. Restore the old keystore and truststore specific to the primary server and the secondary server.

3. Install the NNM iSPI for MPLS on both primary and secondary servers following the steps discussed in Scenario 1.

4. Install the licenses available for the NNM iSPI for MPLS installed on a server 1 and a server 2.

5. Configure the NNM iSPI for MPLS for an application failover.

6. Configure NNMi in the application failover mode. Follow instructions from the *NNMi Deployment Reference Guide* to configure NNMi in an application failover mode

Note: Remove the iSPI for application failover by using the following steps:

1. Disable application failover for the NNM iSPI for MPLS following the steps discussed in the *Disabling NNMi for Application Failover* section in the *NNMi Deployment Reference Guide*.

2. Restore the keystore and the truststore for the systems that you backed up before configuring them for application failover.

Deploy the NNM iSPI for MPLS in an Application Failover Environment with Embedded Database

Scenario 1: In this scenario, consider that you want to install the NNM iSPI for MPLS and NNMi in an application failover mode:

1. Install the NNM iSPI for MPLS and NNMi on the primary server and the secondary server.

2. After the installation of the NNM iSPI for MPLS, install the NNM iSPI for MPLS license on one server and non production licence on the other server.

3. Follow instructions documented in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode. After this, the NNM iSPI for MPLS automatically gets configured in the application failover mode.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for MPLS after configuring NNMi in the application failover mode:

1. Remove the NNMi application failover configuration from the primary and secondary nodes.

2. Restore the old keystore and truststore specific to the primary server and the secondary server configured. See the *NNMi Deployment Reference Guide* for instructions.

3. Install the NNM iSPI for MPLS on both the primary and the secondary servers.

4. Install the NNM iSPI for MPLS license on one server and non production licence on the other server.

5. Follow instructions documented in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode. After this, the NNM iSPI for MPLS automatically gets configured in the application failover mode.

Patching the NNM iSPI for MPLS in an Application Failover Environment

If you have already configured the NNMi and NNM iSPI for MPLS to work in an application failover environment, you must follow this section to apply necessary patches (for both NNMi and NNM iSPI for MPLS).

Both NNMi management servers must be running the same NNMi version and patch level. To add patches to the active and standby NNMi management servers, use the below procedure:

Applying Patches for Application Failover (Shut Down Both Active and Standby)

You can use this procedure when you are not concerned with an interruption in network monitoring.

This procedure results in both NNMi management servers being non-active for some period of time during the patch process. To apply patches to the NNMi management servers configured for application failover, follow these steps:

1. As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see *NNMi Backup and Restore Tools* in the *NNMi Deployment Reference*.

2. As a precaution, on the active NNMi management server, do the following steps:

   a. Run the `nnmcluster` command.

   b. Embedded database only: After NNMi prompts you, type `dbsync`, then press Enter. Review the displayed information to make sure it includes the following messages:

      `ACTIVE_DB_BACKUP:` This means that the active NNMi management server is performing a new backup.

      `ACTIVE_NNM_RUNNING:` This means that the active NNMi management server completed the backup referred to by the previous message.

      `STANDBY_READY:` This shows the previous status of the standby NNMi management server.

      `STANDBY_RECV_DBZIP:` This means that the standby NNMi management server is receiving a new backup from the active NNMi management server.

      `STANDBY_READY:` This means that the standby NNMi management server is ready to perform if the active NNMi management server fails.

3. Run the `nnmcluster -halt` command on the active NNMi management server. This shuts down all `nnmcluster` processes on both the active and standby NNMi management servers.

4. To verify there are no `nnmcluster` nodes running on either server, complete the following steps on both the active and standby NNMi management servers.

   a. Run the `nnmcluster` command.

   b. Verify that there are no `nnmcluster` nodes present except the one marked (SELF).

   c. Run exit or quit to stop the interactive `nnmcluster` process you started.

5. On the active NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.

   a. Edit the following file:

      On Windows:

      %NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties

      On Linux:

      opt/OV/shared/nnm/conf/props/nms-cluster.properties

   b. Comment out the `com.hp.ov.nms.cluster.name` parameter.

   c. Save your changes.

6. Apply the NNMi and the NNM iSPI for MPLS patch to the active NNMi management server using the instructions provided with the patch.

7. On the active NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.

   a. Edit the following file:

      On Windows:

      %NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties

      On Linux:

      opt/OV/shared/nnm/conf/props/nms-cluster.properties

   b. Uncomment the `com.hp.ov.nms.cluster.name` parameter.

   c. Save your changes.

8. Run the `nnmcluster –daemon` command on the active NNMi management server.

9. Run the `nnmcluster -dbsync` command to create a new backup.

10. On the standby NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.

11. Apply the NNMi and the NNM iSPI for MPLS patch to the standby NNMi management server.

12. On the standby NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file

13. Run the `nnmcluster -daemon` command on the standby NNMi management server.

Deploy the NNM iSPI for MPLS with the NNM iSPI for IP Multicast

The NNM iSPI for MPLS helps you to monitor the Provider Edge (PE) routers discovered in a Multicast VPN (MVPN) topology. The PE routers are configured with the multicast-enabled VRF (MVRF) capabilities and use the multicast services to transmit data.

The iSPI for IP Multicast helps you to monitor the multicast services in the network. If the multicast services are used over an MPLS cloud, the integration of the NNM iSPI for MPLS and NNM IP Multicast provides the collaborative monitoring of MVPN topology.

Navigate from the NNM iSPI for MPLS to the NNM iSPI for IP Multicast to view the multicast tree used by multicast traffic in the core network (cloud between the PE routers). The multicast tree shows the default and data Multicast Distribution Tree (MDTs). For more information, *see NNM iSPI for MPLS Online Help, Overview of the Multicast VPN (MVPN) and MPLS view.*

For more information about launching the MPLS views, see NNM IP Multicast View from the *NNM iSPI for MPLS Online Help.*

To deploy the NNM iSPI for MPLS with the (HP) iSPI for IP Multicast, follow the steps:

1. Install NNMi.

2. Install the NNM iSPI for MPLS.

3. Install the NNM iSPI for IP Multicast.

There is no order to deploy the iSPIs (NNM iSPI for MPLS or NNM iSPI for IP Multicast) on a management server.

Deploy the NNM iSPI for MPLS with the NNM iSPI Performance for Quality Assurance

The NNM iSPI for MPLS helps you to monitor the VRFs available on the network. The iSPI Performance for Quality Assurance measures the network traffic performance by configuring various tests on the VRFs. After installing the iSPI Performance for Quality Assurance, the NNM iSPI for MPLS uses the QA performance capabilities. You can view the tests configured for the selected VRF by navigating to the VRF form.

The integration of the NNM iSPI for MPLS and NNM iSPI Performance for QA enables you to do the following:

- View the tests configured on VRFs. Troubleshoot the connectivity for the selected VRFs on basis of the configured tests. For example, finding the quality of connectivity for the multiple sites.

- Troubleshoot the PE-PE, PE-CE, CE-CE connectivity.

- Generate the reports based on the QA metrics. For example, find out the delay for data packet to reach the destination or the packet loss.

For more information, see *Help for iSPI Performance for QA.*

You must deploy NNM iSPI Performance for QA and NNM iSPI for MPLS on the same NNMi management server.

Deploying the NNM iSPI for MPLS with Route Analytics Management System

HP Route Analytics Management System (RAMS) integrates with NNMi to provide the routing protocol path for the layer 3 topology. You can use the RAMS features and functionality to monitor the L3 VPNs that uses the mBGP protocol. In addition, you can use the RAMS capabilities to draw the MPLS path

within MPLS cloud. After the integration with RAMS, you can monitor and view the SNMP traps from the RAMS appliance in the **RAMS** tab. The RAMS tab appears in the **L3 VPN** form. After RAMS is installed, you can push VPN name and RT list to RAMS system by using the `nmsmplsvpnandrtlist.ovpl` tool. For more information, see *NNM iSPI for MPLSOnline Help and NNM iSPI for MPLS Reference Pages.*

Deploy the NNM iSPI for MPLS in Global Network Management Environment

You can deploy the NNM iSPI for MPLS in a Global Network Management (GNM) environment. The NNM iSPI for MPLS uses the capabilities of NNMi Global Network Manager (NNMi GNM) and provides a centralized view to monitor the multiple sites. The NNM iSPI for MPLS allows you to configure the Regional Manager connections by using the `MPLS Configuration` workspace. After the connection is established, view and monitor the MPLS nodes from the NNM iSPI for MPLS inventory (GNM). For more information about how to configure the NNM iSPI for MPLS regional managers, see the *iSPI for MPLS Online Help.*

You can deploy NNMi and NNM iSPI for MPLS in a GNM environment for the following scenarios:

- Both NNMi and NNM iSPI for MPLS are configured on the Global Network Manager server and Regional Manager management servers.

- NNMi is configured on the Global Network Manager server and NNMi and NNM iSPI for MPLS are configured on the Regional Manager management servers.

- Both NNMi and NNM iSPI for MPLS are configured on the Global Network Manager server and NNMi is configured on the Regional Manager management server.

Deploying NNMi and NNM iSPI for MPLS on the Global Network Manager and Regional Manager Management Server

You can install and configure NNMi and the NNM iSPI for MPLS on the Global Network Manager and Regional Managers. For information about the configuration steps, see *NNMi and NNM iSPI for MPLS Online Help.*

The following figure represents a deployment scenario, where NNMi and NNM iSPI for MPLS are configured on the Global Network Manager (G1) and Regional Managers (R1, R2, and R3):

In this deployment scenario, all the Regional Managers (R1, R2, and R3) send the MPLS information to the Global Network Manager (G1). You can view the following information from G1:
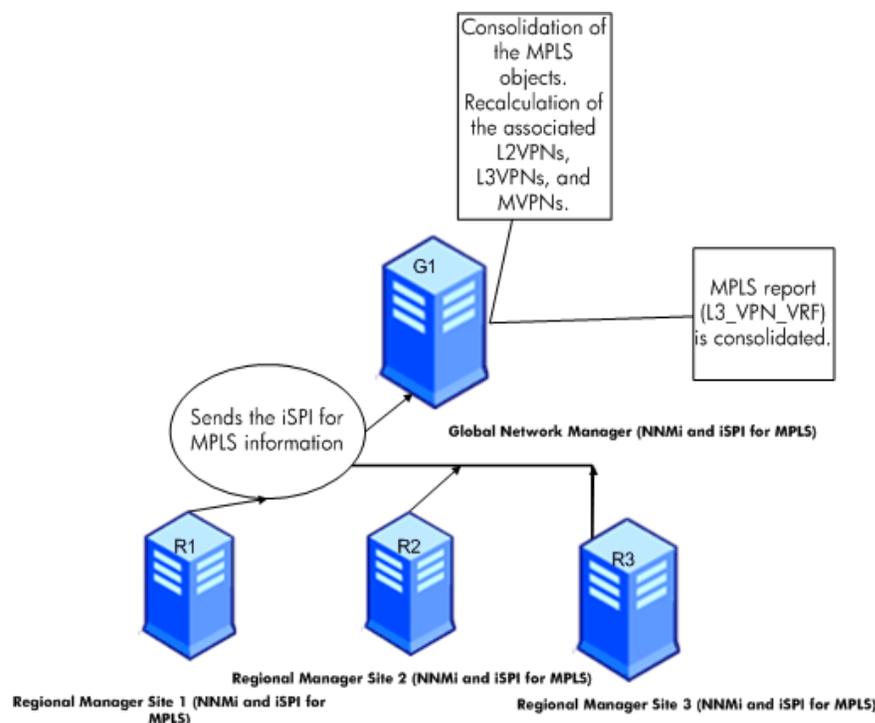
- Consolidated MPLS topology is available. The regional managers send the information about the MPLS objects such as VRFs, TE Tunnels, VC LSPs, and MVRFs to the Global Network Manager (G1). The GNM uses the MPLS object related information from the regional managers to regroup and form the L3 VPNs, L2VPNs, MVPNs, and PseudoWire VCs in the network. In the G1 inventory, the status is recalculated for the MPLS objects. In addition, the incidents are also generated for the MPLS topology in the GNM (G1). The incidents are not forwarded from the regional managers to GNM (G1) as the MPLS topology is derived again in the G1. The incidents are only generated for the MPLS objects available in the G1 inventory.
- Consolidated L3_VPN_VRF report is available. Other MPLS reports are available only for the local MPLS nodes in the G1.

  Note: This is possible only after integrating with NNM iSPI Performance for Metrics.

Deploying NNMi on the Global Network Manager and NNMi and NNM iSPI for MPLS on the Regional Manager Management Server

You can install and configure NNMi on the Global Network Manager and both NNMi and NNM iSPI for MPLS on the Regional Managers. For information about the configuration steps, see the *NNMi and NNM iSPI for MPLS Online Help.*

The following figure represents a deployment scenario, where NNMi is configured on the Global Network Manager (G1). NNMi and the iSPI for MPLS are configured on the Regional Managers (R1, R2, and R3):
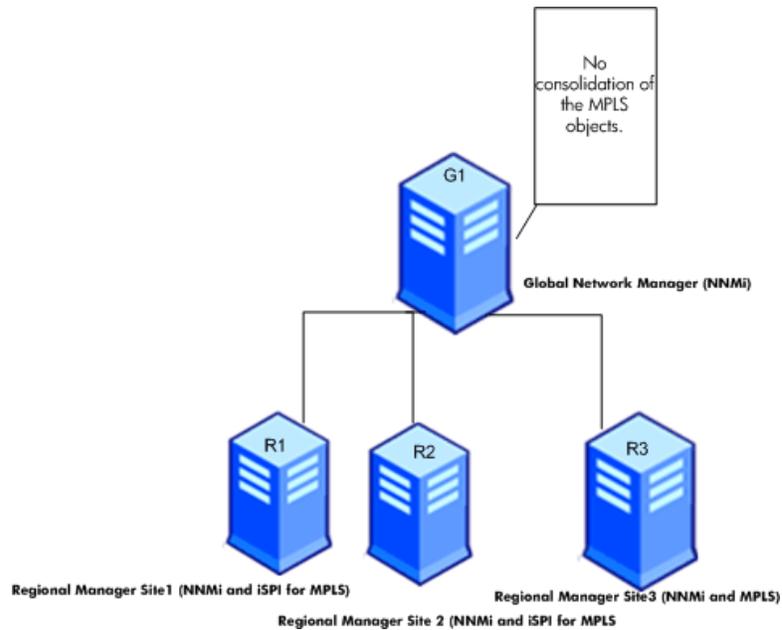
In this deployment scenario, all the Regional Managers (R1, R2, and R3) discover the MPLS nodes and objects such as VRFs, TE Tunnels, VC LSPs, and MVRFs. The NNM iSPI for MPLS is not available on G1 so there is no communication established between G1 and regional managers for the NNM iSPI for MPLS. Thus, the MPLS nodes and objects from the Regional Managers are not available in the G1 inventory. In addition, no aggregated MPLS reports are available in the MPLS (GNM) inventory.

Deploying NNMi and NNM iSPI for MPLS on the Global Network Manager and NNMi on the Regional Manager Management Server

You can install and configure NNMi and the NNM iSPI for MPLS on the Global Network Manager and only NNMi on the Regional Managers. For information about the configuration steps, see in the *NNMi and NNM iSPI for MPLS Online Help.* The following figure represents a deployment scenario, where NNMi and NNM iSPI for MPLS is configured on the Global Network Manager (G1) and NNMi on the Regional Managers (R1, R2, and R3):
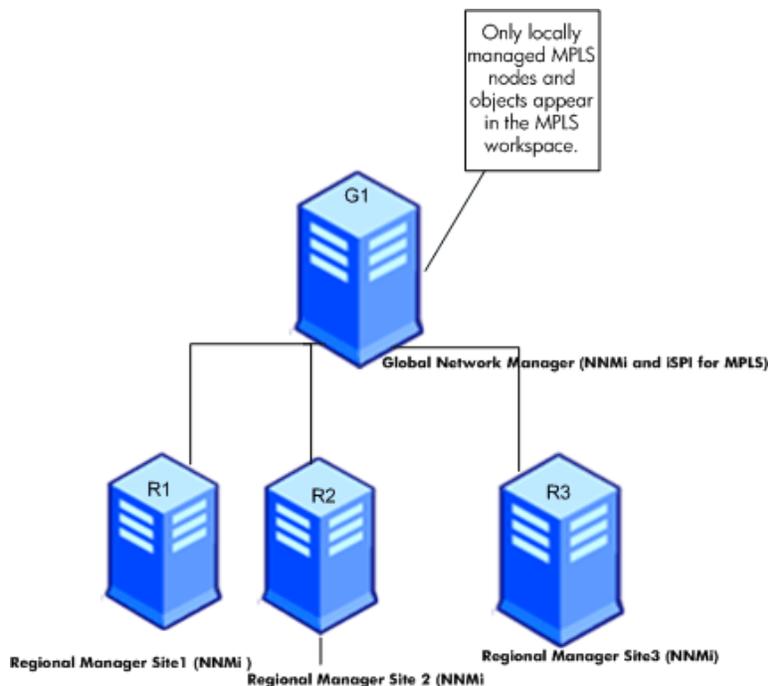
In this deployment scenario, only the locally managed MPLS nodes and objects such as L3 VPNs, L2VPNs, MVPNs, and PseudoWire VCs are available in the MPLS inventory (G1).

Deploying the Regional Manager in the Application Failover Environment

When the NNM iSPI for MPLS Regional Manager is in the Application failover environment, use the **ORDER** parameter to decide the priority to establish the connection.

To use the regional manager in an application failover environment, follow these steps:

1. Configure the Regional Manager connection using MPLS configuration workspace.
2. Add the two regional manager connections and provide the two hostnames.
3. Use the **ORDER** parameter to give different values to the two regional managers.

Whenever there is an application fail-over available on the regional manager, the GNM will always use the lowest order value to establish the next connection.

You can configure the regional manager in the application failover environment by using the steps documented in the following:

- "Deploy the NNM iSPI for MPLS in an Application Failover Environment with Oracle Database" on page 15
- "Deploy the NNM iSPI for MPLS in an Application Failover Environment with Embedded Database" on page 16.

Chapter 3: Installing the NNM iSPI for MPLS in an HA Cluster

You can install NNMi and NNM iSPI for MPLS in a High Availability (HA) environment to achieve redundancy in your monitoring setup. The prerequisites to configure the NNM iSPI for MPLS in an HA environment is similar to NNMi. For information, see *NNMi Deployment Reference* .

Installing the NNM iSPI for MPLS

You can configure the NNM iSPI for MPLS for the following scenarios:

Install NNMi and the NNM iSPI for MPLS in your environment before configuring NNMi to run under HA. See "Configuring an HA Cluster on a Set of Systems with NNMi and iSPI for MPLS" below.

Install and configure the NNM iSPI for MPLS in an existing NNMi HA cluster environment. See "Installing the NNM iSPI for MPLS in an Existing NNMi HA Cluster Environment" on page 26.

> **Note:** To configure PKI authentication on the NNM iSPI for MPLS in an HA cluster, you must perform all the required changes on both, primary and secondary node. For information on required changes, see "Configuring Access with Public Key Infrastructure Authentication" on page 11.

Configuring an HA Cluster on a Set of Systems with NNMi and iSPI for MPLS

If you have NNMi and the NNM iSPI for MPLS installed on at least two systems, you can create an HA cluster and configure NNMi and the iSPI for MPLS to run under HA.

You can configure NNMi and NNM iSPI for MPLS on the primary node and secondary node in an HA environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference*.

Configure the NNM iSPI for MPLS on the Primary Node

To configure the NNM iSPI for MPLS on the primary node, follow these steps:

1. Install NNMi and NNM iSPI for MPLS on each system. See the *NNMi Installation Guide* and the *NNM iSPI for MPLS Installation* guide for more information.

2. Configure the HA software on the systems and configure NNMi to run under HA. See the *NNMi Deployment Reference* for information on configuring NNMi to run under HA. Do not start the

resource group while configuring NNMi to run under the HA (do not run the `nnmhastartrg.ovpl` command).

3. Configure the NNM iSPI for MPLS on the primary (active) node:

   a. Run the following command to find the virtual hostname:

      `nnmofficialfqdn.ovpl`

   b. Modify the following files from the file from the *$NnmdataDir*/shared/mpls/conf or *%NnmdataDir%*\shared\mpls\conf to replace the host name with the virtual FQDN for the following parameters:

File Name	Variable Name
`nms-mpls.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.spi.hostname`

   c. Modify the server.properties file from the %nnminstalldir%\mpls\server\ or /opt/OV/mpls/server/ directory to reflect the Virtual FQDN of the NNMi management server for the com.hp.ov.nms.fqdn parameter.

   d. Modify the `login-config.xml` file from the %nnminstalldir%\mpls\server\conf or /opt/OV/mpls/server/conf directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

   e. Run the following command to start the NNMi HA resource group:

      For Windows:

      `%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <resource_group>`

      For Linux:

      `/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl NNM <resource_group>`

      For more information, see *NNMi Deployment Reference* guide.

      The NNM iSPI for MPLS and NNMi must start after this step. If NNMi or the NNM iSPI for MPLS does not start, see *Troubleshooting the HA Configuration* from *NNMi Deployment Reference*.

   f. Run the following command to configure the NNM iSPI for MPLS to run under the HA cluster:

      For Windows:

      `%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS`

      For Linux:

      `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS`

4. Configure the NNM iSPI for MPLS on the secondary (passive) node:

   a. Install NNMi with NNM iSPI for MPLS on the secondary node. Make sure the secondary node has a separate Fully Qualified Domain Names (FQDN) during the installation. See the *NNMi Installation Guide* and the *HP Network Node Manager iSPI Performance for MPLS Software Installation* guide for more information.

   b. Run the following command to find the virtual hostname:

```
nnmofficialfqdn.ovpl
```

c. Modify the following files in the *$NnmdataDir*/shared/mpls/conf or
   %NnmdataDir%\shared\mpls\conf to replace the host name with the virtual FQDN for the
   following parameters:

File Name	Variable Name
nms-mpls.jvm.properties	-Dnmsas.server.security.keystore.alias
nnm.extended.properties	com.hp.ov.nms.spi.mpls.Nnm.hostname
nnm.extended.properties	com.hp.ov.nms.spi.mpls.spi.hostname

d. Modify the server.properties file from the %nnminstalldir%\mpls\server\ or
   /opt/OV/mpls/server/ directory to reflect the Virtual FQDN of the NNMi management server
   for the com.hp.ov.nms.fqdn parameter.

e. Modify the login-config.xml file from the %nnminstalldir%\mpls\server\conf or
   /opt/OV/mpls/server/conf directory to reflect the virtual FQDN of the NNMi management
   server (for the module-option element).

f. Run the following commands to configure the NNM iSPI for MPLS on the secondary node to
   run under the HA cluster:

   For Windows:

   %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS

   For Linux:

   /opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS

5. Repeat step 4 if you have additional passive nodes in the HA cluster.

Installing the NNM iSPI for MPLS in an Existing NNMi HA Cluster Environment

You can configure the NNM iSPI for MPLS on the primary node and secondary node in an NNMi HA
cluster environment. For more information on how to install NNMi in an HA environment, see *NNMi
Deployment Reference* guide.

1. Make sure that NNMi is running on the primary server.

2. Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under
   the following directory:

   %nnmdatadir%\hacluster*<resource_group_name>*

   $NnmDataDir/hacluster/*<resource_group_name>*

3. Run ovstatus -c ovjboss to make sure that ovjboss is running.

4. Install the NNM iSPI for MPLS on the primary (active) node in the cluster, but do *not* start the
   NNM iSPI for MPLS.

5. Modify the following files from the *$NnmdataDir*/shared/mpls/conf or

`%NnmdataDir%\shared\mpls\conf` to replace the host name with the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-mpls.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.spi.hostname`

6. Modify the server.properties file from the %nnminstalldir%\mpls\server\ or /opt/OV/mpls/server/ directory to reflect the Virtual FQDN of the NNMi management server for the com.hp.ov.nms.fqdn parameter.

7. Modify the `login-config.xml` file from the `%nnminstalldir%\mpls\server\conf` or `/opt/OV/mpls/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

8. If you have modified any of the following folders or files, replicate them on each cluster member.

   For Linux:

   `/opt/OV/mpls/server/conf/`

   `/var/opt/OV/shared/mpls/conf/`

   `/opt/OV/mpls/server/deploy/jboss-logging.xml`

   `/var/opt/OV/nmsas/mpls/conf/nms-auth-config.xml`

   `/var/opt/OV/nmsas/mpls/server.properties`

   `/opt/OV/mpls/server/server.properties`

   For Windows:

   `%NnmInstallDir%\mpls\server\conf\`

   `%NnmDataDir%\shared\mpls\conf\`

   `%NnmInstallDir%\mpls\server\deploy\jboss-logging.xml`

   `%NnmDataDir%\nmsas\mpls\conf\nms-auth-config.xml`

   `%NnmDataDir%\nmsas\mpls\server.properties`

   `%NnmInstallDir%\mpls\server\server.properties`

   > **Note:** Make sure the `.keyFile` created after adding the NON SNMP credentials on active or passive servers under `/var/opt/OV/shared/mpls/conf/` or `%NnmDataDir%\shared\mpls\conf` is copied to all the passive servers.

9. Remove the `maintenance` file that you added in step 2

10. Initiate a failover to a secondary (passive) node in the cluster where you want to install the NNM iSPI for MPLS. Make sure that NNMi fails over and runs on the secondary server successfully.

11. On this system, follow these steps:

    a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

%nnmdatadir%\hacluster*<resource_group_name>*

$NnmDataDir/hacluster/*<resource_group_name>*

b. Run `ovstatus -c ovjboss` to make sure that `ovjboss` is running.

c. Install the NNM iSPI for MPLS on this server., but do *not* start the iSPI.

> **Note:** The NNM iSPI for MPLS displays two error messages: `create db user` and `create DB`. Ignore these errors and continue with the installation.

d. Modify the following files in the file from the `/var/opt/OV/shared/mpls/conf` or *%NnmdataDir%*\shared\mpls\conf   to replace the host name with the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-mpls.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.spi.hostname`

e. Modify the server.properties file from the %nnminstalldir%\mpls\server\ or /opt/OV/mpls/server/ directory to reflect the Virtual FQDN of the NNMi management server for the com.hp.ov.nms.fqdn parameter.

f. Modify the `login-config.xml` file from the %nnminstalldir%\mpls\server\conf or /opt/OV/mpls/server/conf directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

g. If you have modified any of the following folders or files, replicate them on each cluster member.

For Linux:

/opt/OV/mpls/server/conf/

/var/opt/OV/shared/mpls/conf/

/opt/OV/mpls/server/deploy/jboss-logging.xml

/var/opt/OV/nmsas/mpls/conf/nms-auth-config.xml

/var/opt/OV/nmsas/mpls/server.properties

/opt/OV/mpls/server/server.properties

For Windows:

%NnmInstallDir%\mpls\server\conf\

%NnmDataDir%\shared\mpls\conf\

%NnmInstallDir%\mpls\server\deploy\jboss-logging.xml

%NnmDataDir%\nmsas\mpls\conf\nms-auth-config.xml

%NnmDataDir%\nmsas\mpls\server.properties

%NnmInstallDir%\mpls\server\server.properties

> **Note:** Make sure the `.keyFile` created after adding the NON SNMP credentials on active or passive servers under `/var/opt/OV/shared/mpls/conf/` or `%NnmDataDir%\shared\mpls\conf` is copied to all the passive servers.

    h. Remove the `maintenance` file that you added in step a.

12. If you have multiple nodes in the cluster, fail over to another passive server, and then repeat step a through step h.

13. You must fail over to the server that was active when you started with this procedure.

14. Run the following command on the active server first, and then on all passive servers:

    For Windows:

    `%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS`

    For Linux:

    `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS`

15. Verify that the NNM iSPI for MPLS is successfully registered by running the following command:

    On Windows:

    `%nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –config NNM –get NNM_ADD_ON_PRODUCTS`

    On Linux:

    `/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –config NNM –get NNM_ADD_ON_PRODUCTS`

Patching the NNM iSPI for MPLS in an HA Cluster

If you have already configured NNMi and the NNM iSPI for MPLS to work in an HA cluster, you must follow this section to apply necessary patches (for both NNMi and the NNM iSPI for MPLS).

To apply patches for NNMi and NNM iSPI for MPLS, follow these steps:

1. Determine which node in the HA cluster is active:

    Windows:

    `%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl`

    `-group <resource_group> -activeNode`

    Linux:

    `/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl`

    `-group <resource_group> -activeNode`

2. On the active node, put the NNMi HA resource group into maintenance mode by creating the following files:

    Windows:

    `%NnmDataDir%\hacluster\<resource_group>\maintenance`

    `%NnmDataDir%\hacluster\<resource_group>\maint_NNM`

    Linux:

    `/var/opt/OV/hacluster/<resource_group>/maintenance`

```
/var/opt/OV/hacluster/<resource_group>/maint_NNM
```

Include the NORESTART keyword in both these files.

3. On all passive nodes, put the NNMi HA resource group into maintenance mode by creating the following files:

   Windows:

   ```
   %NnmDataDir%\hacluster\<resource_group>\maintenance
   ```

   ```
   %NnmDataDir%\hacluster\<resource_group>\maint_NNM
   ```

   Linux:

   ```
   /var/opt/OV/hacluster/<resource_group>/maintenance
   ```

   ```
   /var/opt/OV/hacluster/<resource_group>/maint_NNM
   ```

   Include the NORESTART keyword in both these files.

4. On the active node, follow these steps:

   a. Stop NNMi:

      ```
      ovstop -c
      ```

   b. Back up the shared disk by performing a disk copy.

   c. Use the nnmbackup.ovpl command or another database command to backup all NNMi data. For example

      ```
      nnmbackup.ovpl -type offline -scope all -target nnmi_backups
      ```

      For more information about this command, see *NNMi Backup and Restore Tools* section in the *NNMi Deployment Reference*.

   d. Apply the appropriate NNMi and NNM iSPI patches to the system.

   e. Start NNMi:

      ```
      ovstart -c
      ```

   f. Verify that NNMi started correctly:

      ```
      ovstatus -c
      ```

      All NNMi services should show the state RUNNING.

5. On each passive node, apply the appropriate patches to the system.

6. On all passive nodes, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from the nodes.

7. On the active node, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from that node.

Unconfiguring the NNM iSPI for MPLS in an HA cluster

To unconfigure the NNM iSPI for MPLS in an HA cluster, follow these steps:

1. Determine which node in the HA cluster is active. On any of the HA cluster node, run the following command:

On Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <resource_group> -
activeNode
```

On Linux

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <resource_group> -
activeNode
```

2. On each passive node, unconfigure the NNM iSPI for MPLS add-on from the HA cluster. To unconfigure, run the following command:

   On Windows

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon MPLS
   ```

   On Linux

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon MPLS
   ```

3. Verify that the NNM iSPI for MPLS add-on is unconfigured on all the cluster passive nodes. To verify, run the following command:

   On Windows

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
   PRODUCTS
   ```

   On Linux

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
   PRODUCTS
   ```

   If any passive cluster node with the NNM iSPI for MPLS add-on appears in the output, repeat step 2 on that node.

4. You can now unconfigure the NNM iSPI for MPLS from the HA cluster on the active node. To unconfigure, run the following command:

   On Windows

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon MPLS
   ```

   On Linux

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon MPLS
   ```

5. Make sure that NNMi is running on the active node.

6. Verify that ovjboss is running by using the following command:

   ```
   ovstatus -c ovjboss
   ```

7. Uninstall the NNM iSPI for MPLS from the active node. For more information see, *Removing the NNM iSPI for MPLS* section in the *Installation Guide*.

8. After you uninstall, failover to passive node. Make sure that NNMi fails over and runs on the secondary server successfully.

9. Verify that ovjboss is running by using the following command:

   ```
   ovstatus -c ovjboss
   ```

10. Uninstall the NNM iSPI for MPLS from the secondary nodes. For more information see, *Removing the NNM iSPI for MPLS* section in the *Installation Guide*.

   Note: You can ignore the database related warning messages while uninstalling the NNM

iSPI for MPLS.

11. After you uninstall the NNM iSPI for MPLS from the secondary node, failback to primary node.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Deployment Reference (Network Node Manager iSPI for MPLS 10.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback!